IX kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 96)**
- **Komisji Spraw Zagranicznych (nr 133)**

z dnia 9 marca 2023 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 96)

Komisji Spraw Zagranicznych (nr 133)

9 marca 2023 r.

Komisje: Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Spraw Zagranicznych, obradujące pod przewodnictwem posła **Radosława Fogla (PiS)**, przewodniczącego Komisji Spraw Zagranicznych, rozpatrzyły:

– informację na temat przygotowania państwa na płynące z zagranicy zagrożenia związane z cyberprzestępczością.

W posiedzeniu udział wzięli: **Paweł Jabłoński** podsekretarz stanu w Ministerstwie Spraw Zagranicznych wraz ze współpracownikami, **Paweł Lewandowski** podsekretarz stanu w Kancelarii Prezesa Rady Ministrów wraz ze współpracownikami, **Jacek Kosiorek** i **Paweł Łuczak** wiceprezesi Polskiej Izby Radiodyfuzji Cyfrowej, **Wojciech Maciejczak** członek Polskiej Izby Informatyki i Telekomunikacji, **Marta Kokoszka** członek Związku Pracodawców Technologii Cyfrowych Lewiatan oraz **Joanna Karczewska** członek Stowarzyszenia ISACA Warszawa.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Marta Artymińska**, **Marcin Chorzewski**, **Magdalena Krzymowska**, **Artur Kucharski** i **Wioletta Więciorkowska** – z sekretariatów Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Radosław Fogiel (PiS):

Otwieram wspólne posiedzenie Komisji Spraw Zagranicznych oraz Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Witam bardzo serdecznie panie i panów posłów. Witam obecnych przedstawicieli rządu – pana ministra Pawła Jabłońskiego, podsekretarza stanu w Ministerstwie Spraw Zagranicznych, wraz ze współpracownikami oraz pana ministra Pawła Lewandowskiego, podsekretarza stanu w Kancelarii Prezesa Rady Ministrów, wraz ze współpracownikami. Witam pozostałych gości – przedstawicieli organizacji, którzy uczestniczą w naszym posiedzeniu.

Na podstawie listy obecności stwierdzam kworum.

Porządek dzienny państwo otrzymali. Obejmuje on punkt: „Informacja na temat przygotowania państwa na płynące z zagranicy zagrożenia związane z cyberprzestępczością”. Jeśli nie usłyszę sprzeciwu, uznam porządek za przyjęty. Nie słyszę. Dziękuję serdecznie.

Przystępujemy zatem do jego rozpatrzenia. Dostałem sygnał, że pan minister Jabłoński może mieć później inne zobowiązania, więc poprosiłbym pana ministra jako pierwszego o zabranie głosu i przedstawienie tematu z punktu widzenia MSZ. Bardzo proszę, panie ministrze.

Podsekretarz stanu w Ministerstwie Spraw Zagranicznych Paweł Jabłoński:

Bardzo dziękuję. Panie przewodniczący, Wysokie Komisje, panie ministrze, szanowni państwo, rzeczywiście postaram się skrótowo przedstawić stanowisko MSZ w tej sprawie, choć zaznaczę na początku, że MSZ jako takie nie ma bezpośrednich kompetencji ustawowych. Prowadzi oczywiście działania w kontekście nawiązywania współpracy z partnerami zagranicznymi i dialogów politycznych. Robimy to zarówno w ramach Unii Europejskiej i Sojuszu Północnoatlantyckiego (NATO), jak i w procesach innych organizacji wielostronnych, a także w ramach stosunków dwustronnych.

W ramach procesów międzynarodowych kluczowym dokumentem z zakresu przeciwdziałania cyberprzestępczości jest konwencja Rady Europy o cyberprzestępczości, zwana konwencją budapesztańską. To jest konwencja z 2001 r., którą Polska jest związana od 2015 r. Określa ona m.in. znamiona tzw. przestępstw komputerowych i procedury postępowania w związanych z nimi sprawach. Państwa – strony konwencji są zobowiązane do jej wdrożenia. Polska to zobowiązanie wykonała. Odpowiednie typy przestępstw zostały wpisane do polskiego Kodeksu karnego.

Ponadto na mocy rezolucji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych (ZO ONZ) nr 74/247 z 2019 r. rozpoczął się proces negocjacji kolejnego instrumentu prawnego, a mianowicie kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu informacji i technologii komunikacyjnych do celów przestępczych. Te prace koncentrują się na takich kwestiach jak zagadnienia dotyczące kryminalizacji i działania organów ścigania, środki procedur karnych, definicje pewnych pojęć, żeby one były ujednolicone. Na tym etapie właśnie ta kwestia jest jeszcze omawiana. Są różne pomysły na to, jak te pojęcia powinny być zdefiniowane i jaki powinien być zakres przedmiotowy tej konwencji. Tutaj oczywiście, ponieważ jest to forum ZO ONZ, to różne pomysły zgłaszają także takie państwa jak np. Federacja Rosyjska. Musimy sobie z tego zdawać sprawę, że w tym procesie ma miejsce również ten aspekt, a zatem proces jest dość złożony i trudny. Natomiast choć są trudności i mogą się pojawiać pomysły na to, jak rozwadniać ochronę międzynarodową, to w ocenie MSZ warto jest dążyć do tego, aby konwencja została przyjęta.

Ponadto jest również takie ciało jak Komitet Ad Hoc (AHC) w ramach negocjacji tej konwencji. Polska jest tam reprezentowana przez przedstawicieli Ministerstwa Sprawiedliwości, MSZ, Prokuratury Krajowej. Posiedzenia AHC odbywają się z różną regularnością. Ostatnie było w marcu ubiegłego roku. Natomiast założenie jest takie, że przygotowanie tekstu konwencji ma nastąpić na początku przyszłego roku, w styczniu–lutym 2024 r.

Znaczenie dla utrzymania globalnego charakteru debaty na temat cyberbezpieczeństwa mają także prace otwartej grupy roboczej do spraw odpowiedzialnego zachowania państw w cyberprzestrzeni (OEWG). Mandat tej grupy jest przewidziany na lata 2021–2025. To jest kontynuatorka wcześniejszej, podobnej grupy z lat 2019–2021, a także wcześniejszych sześciu edycji grupy ekspertów rządowych w latach 2006–2021. W trzech konsensualnych raportach tych grup ekspertów rządowych zarekomendowano łącznie 11 dobrowolnych, niewiążących form odpowiedzialnego zachowania państw w cyberprzestrzeni, w tym m.in. normę nr 4, czyli współpracę partnerów w zakresie wymiany informacji i przeciwdziałania cyberprzestępczości. Polska w takich działaniach uczestniczy, choćby w kontekście udziału polskiej Policji w grupie *Joint Cybercrime Action Taskforce* (J-CAT) w ramach Europolu.

Z polskiej inicjatywy we współpracy z Królestwem Niderlandów rozpoczęte zostały też prace na forum UE w zakresie rewizji podstawowego narzędzia unijnego odnośnie do politycznej reakcji na cyberataki przeciw UE i państwom członkowskim, czyli tzw. *Cyber Diplomacy Toolbox*. Polska postuluje wzmocnienie mechanizmów sankcyjnych w odpowiedzi na ataki. Proponujemy dodanie możliwości nakładania sankcji sektorowych na państwa, które nie tylko prowadzą bezpośrednie ataki, ale także te, które swoją polityką ułatwiają czy też wspierają działania grup przestępczych mieszczących się czy działających z wykorzystaniem terytoriów tych państw.

Ponadto w 2020 r. z inicjatywy MSZ rząd przyjął stanowisko dotyczące stosowania prawa międzynarodowego w cyberprzestrzeni. Również w ten sposób rząd Rzeczypospolitej Polskiej podkreśla, że poszanowanie dla prawa międzynarodowego i dla norm międzynarodowych jest niezbędnym warunkiem utrzymania międzynarodowego pokoju i bezpieczeństwa między państwami, także właśnie w cyberprzestrzeni. Dotyczy to też obowiązku państwa w zakresie przeciwdziałania na swoim terytorium działaniom przestępczym.

Na zakończenie warto wspomnieć o inicjatywie rządów Stanów Zjednoczonych i międzynarodowej współpracy w zakresie zwalczania szerzącego się zjawiska wymuszania okupów za przejęte dane, czyli *Counter Ransomware Initiative*. Taka

inicjatywa się pojawiła się w 2021 r. W pracach grupy roboczej uczestniczą nasi eksperci z MSZ. To grupa cyberdyplomacji mająca usprawnić koordynację reakcji państw partnerskich na poziomie polityczno-dyplomatycznym, w tym przede wszystkim koordynację wspólnych odpowiedzi na cyberataki.

To tyle z mojej strony. Myślę, że pan minister Lewandowski chętnie uzupełni. Bardzo dziękuję.

Przewodniczący poseł Radosław Fogiel (PiS):

Bardzo dziękuję, panie ministrze. Bardzo proszę pana ministra Lewandowskiego o zabranie głosu.

Podsekretarz stanu w Kancelarii Prezesa Rady Ministrów Paweł Lewandowski:

Dziękuję bardzo. Oczywiście chętnie uzupełnię. Spotykamy się w 379 dniu agresji Rosji na Ukrainę – inwazji, która zmieniła dotychczasowe priorytety i wektory działania. Dziś trudno nie mówić o cyberbezpieczeństwie i dezinformacji, nie odnosząc się do tego, co się dzieje za wschodnią granicą Polski, jak i związanych z tą sytuacją zagrożeń. Mowa tutaj nie tylko o próbach zdestabilizowania czy też zinfiltrowania systemów państwa obranego za cel. To przede wszystkim próby działania od warstwy propagandowej i dezinformacyjnej.

Warto jednak podkreślić, że wojna na Ukrainie nie przyniosła żadnego widocznego osłabienia w obszarze polskiego cyberbezpieczeństwa. Możemy jednak potwierdzić wzrost liczby zagrożeń w tych kategoriach, które korespondują z wydarzeniami za naszą wschodnią granicą. Część z nich to naturalna okazja dla grup aktywistów sympatyzujących ze stroną rosyjską i realizujących proste typy ataków, takie jak DDoS (*Distributed Denial of Service*). Należy jednak zauważyć, że jeżeli w wyniku takiego ataku jakaś usługa była niedostępna, to niedostępność ta była chwilowa i nie powodowała żadnych zagrożeń dla bezpieczeństwa przetwarzanych w niej danych.

Wzrost ataków, o których pisał w swojej interpelacji pan poseł wynika w naszej ocenie nie tylko z sytuacji na Ukrainie, ale także z wyników procesów zachodzących w polskiej przestrzeni. Postępująca cyfryzacja, do której przyczyniła się także pandemia COVID, rozwój automatyki przemysłowej, internet rzeczy, sprzęt mobilny, przeorientowanie się grup przestępczych na działania w obszarze cyberprzestrzeni jako dających większe profity, ale przede wszystkim wzrost świadomości. Dzięki kampaniom edukacyjnym Polacy coraz skuteczniej rozpoznają działania cyberprzestępców i zgłaszają je do właściwych instytucji.

W nawiązaniu do tematu dzisiejszego posiedzenia chciałbym jednak podkreślić, że rząd RP prowadzi działania na rzecz zapewnienia bezpieczeństwa w cyberprzestrzeni, w tym również monitoruje płynące z zagranicy zagrożenia związane z cyberprzestępczością oraz im aktywnie przeciwdziała. W tym kontekście chciałbym odnieść się do następujących zagadnień: *smishing*, domeny internetowe służące wyłudzaniu danych, *spoofing*, *ransomware*, dezinformacja w mediach społecznościowych, DDoS, a także zwalczanie i zapobieganie materiałom przedstawiającym seksualne wykorzystanie dzieci.

Pierwszym z tych zagadnień, czyli *smishingiem*, zajęliśmy się w ramach prac nad projektem ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, który zakłada środki przeciwdziałające tym nadużyciom, inicjowanym również za granicą. Gdyby państwo nie wiedzieli, to są działania polegające na wyłudzaniu przez spreparowane SMS-y danych, pieniędzy czy dostępu do różnych kont. Niezmiennie najpopularniejszy schemat *smishingu* lub *phishingu* – to jest to samo, tylko za pomocą innych metod, np. maila – to próba nakłaniania ofiary do wejścia na stronę z fałszywym panelem płatności i kradzież danych logowania do bankowości internetowej albo danych karty płatniczej. Scenariuszem najczęściej jest dopłata do przesyłki czy niezapłacony rachunek za energię, ale ostatnio obserwujemy również kampanię podszywających się pod serwisy rządowe.

Przedsiębiorcy telekomunikacyjni będą blokować próbki wiadomości SMS zgodne ze wzorcem wiadomości wyczerpującej znamiona *smishingu*, przekazanym przez zespół CSIRT (*Computer Security Incident Response Team*) Narodowej i Akademickiej Sieci Komputerowej. Warto podkreślić, że wiadomości te są inicjowane zarówno

z numerów krajowych, jak i z zagranicznych. W 2021 r. zespół w NASK otrzymał łącznie 18 852 zgłoszenia *phishingu* w polskich sieciach, a można domniemywać, że niezgłoszonych przypadków na pewno było o wiele więcej. Wraz z NASK zachęcamy, aby każdego takiego SMS-a zgłaszać do CSIRT NASK. Teraz można to zrobić jeszcze łatwiej, używając w swoim telefonie funkcji „przekaż” albo „udostępnij”, przesyłając bezpośrednio na odpowiedni numer telefonu. Ponieważ oglądając nasz różni ludzie, to powiem, jaki to jest numer: 799 448 084.

Kolejna inicjatywa umocowana na poziomie ustawowym to lista ostrzeżeń dotyczących domen internetowych, także domen zagranicznych, które służą do wyłudzania danych i środków finansowych użytkowników internetu. Lista ta jest prowadzona również przez CSIRT NASK i dostępna online. Jest tam obecnie wpisanych 87 tys. domen internetowych. Tylko w 2022 r. dzięki jej istnieniu udało się zablokować ponad 20 mln prób wejścia na strony z listy.

Ustawa będzie przeciwdziałać także podszywaniu się oszustów pod numery osób lub instytucji przy wywoływaniu połączenia głosowego, czyli *spoofing*. Ruch ten jest często inicjowany spoza granic Rzeczypospolitej. Przestępcy korzystają w tym celu z internetowych bramek telefonii VoIP (*Voice over Internet Protocol*). Podmioty publiczne będą zobowiązane stosować mechanizmy uwierzytelniania poczty elektronicznej. Rozwiązanie to będzie przeciwdziałało atakom *phishing* na podmioty publiczne, m. in. jednostki samorządu terytorialnego, organy władzy publicznej, w tym organy administracji rządowej, organy ochrony prawa czy uczelnie publiczne.

Kolejnym dużym wyzwaniem jest *ransomware* – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, często poprzez techniki szyfrujące, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego. Programy typu *ransomware* należą do tzw. złośliwego oprogramowania. Polska uczestniczy w pracach grup roboczych *Counter Ransomware Initiative* (CRI). Współpracujemy międzynarodowo w celu dalszego budowania zbiorowej odporności na oprogramowanie *ransomware*, ścigania odpowiedzialnych podmiotów i przeciwdziałania nielegalnemu finansowaniu, które stanowi podstawę ekosystemu oprogramowania *ransomware*. Inicjatywa CRI została uruchomiona w październiku 2021 r. przez amerykańską Radę Bezpieczeństwa Narodowego. Dołączyło do niej 36 krajów, w tym Polska.

W 2022 r. Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów aktywnie uczestniczył w pracach grup roboczych do spraw dyplomacji i partnerstwa publiczno-prywatnego, dzieląc się dobrymi praktykami, opracowując podejścia strategiczne i biorąc wraz z MSZ udział w ćwiczeniach dotyczących budowania odporności państw na ataki typu *ransomware*. Przedstawiciele Polski podzielili się doświadczeniami ze współpracy w ramach „Programu współpracy w cyberbezpieczeństwie” (PWCyber).

Podejmujemy działania, aby skutecznie walczyć ze wspomnianymi atakami DDoS, które w wielu przypadkach jednoznacznie kojarzymy z sytuacją na Ukrainie. Właśnie dlatego uruchomiliśmy projekt anty-DDoS, który kluczowej grupie podmiotów zapewnia parasol ochronny przed atakami. Dodatkowo systemowo sprawdzamy, jakie usługi są wystawiane i widziane na zewnątrz organizacji z internetu. Projekt pod nazwą Artemis prowadzi zespół CSIRT NASK. Cały czas prowadzone jest skanowanie infrastruktury różnych grup podmiotów. Wynikiem tego działania jest wykrycie dużej liczby błędów bezpieczeństwa lub konfiguracji, potencjalnie pozwalających na ingerencję w środowisko przetwarzania danych. Przy współpracy z administratorami odpowiedzialnymi za poszczególne systemy jest to systematycznie naprawiane.

Istotnym elementem podnoszenia poziomu cyberbezpieczeństwa są programy służące zarówno podnoszeniu kompetencji cyfrowych pracowników, jak i niwelowaniu długu technologicznego, który występuje w infrastrukturze IT instytucji, w tym również w zakresie systemów odpowiedzialnych za cyberbezpieczeństwo. Przykładem projektów dedykowanych jednostkom samorządu terytorialnego są „Cyfrowa Gmina” i „Cyfrowy Powiat”. W przygotowaniu są kolejne inicjatywy, które służą bezpośrednio uzupełnieniu braków w infrastrukturze bezpieczeństwa w tych podmiotach czy też zapewnieniu konkretnego wsparcia w usuwaniu skutków incydentów, np. poprzez dostarczenie niezbędnych zasobów sprzętowych IT.

Wyzwaniem jest również dezinformacja w mediach społecznościowych, a źródła przenoszenia zagranicznych linii narracyjnych do polskiej infosfery w głównej mierze pochodziły z rosyjskojęzycznej części mediów społecznościowych. Dużą rolę odgrywał tutaj serwis Telegram. Aby przeciwdziałać dezinformacji, skupiliśmy się na budowaniu skutecznego mechanizmu, który jest nastawiony na obserwowanie i zwalczanie zjawisk szkodliwych w formule *real time*. Do skutecznej walki z dezinformacją potrzebne jest zaangażowanie wielu stron życia publicznego, przede wszystkim polityków, środowiska akademickiego, mediów, organizacji pozarządowych (NGO) i właścicieli platform społecznościowych. Musimy zbudować zaufanie między sobą i dzielić się istotnymi informacjami czy danymi. Żeby skutecznie i wcześnie wyłapywać szkodliwe treści i móc im przeciwdziałać, potrzebujemy danych i wyjęcia tematu dezinformacji z bieżącego sporu politycznego. Dziś przykład ukraiński, który będziemy chcieli zastosować również w Polsce, pokazuje wagę aktywnej obrony w cyberświecie. Dezinformacja, tak jak i inne zagrożenia hybrydowe, są niestety klarowną wskazówką, że funkcjonalnie musimy działać zgodnie z regułami wojennymi. Dlatego też można przeciwdziałać dezinformacji, oddziałując również na drugą stronę i zaszczepiając prawdziwe informacje. Z dezinformacją najlepiej walczyć edukacją. Nie możemy jednak oczekiwać, że przy potopie informacji, jakiego doświadczamy, będziemy nakłaniać ludzi do weryfikacji każdej wiadomości. Musimy budować świadomość, by w istotnych momentach zadziałały pożądane mechanizmy, krytyczne myślenie, szukanie prawdziwych źródeł.

Wdrażane w Polsce główne sposoby przeciwdziałania dezinformacji to m.in. bieżący monitoring mediów społecznościowych, alertowanie szczególnie groźnych przypadków, wykorzystywanie dostępnych narzędzi i baz danych do wyszukiwania szkodliwych treści w przestrzeni mediów społecznościowych, mapowanie i monitorowanie zdiagnozowanych wcześniej kont oraz bieżącej sytuacji w infosferze w kluczowych wątkach. Istotne są również predykcje możliwych linii narracyjnych i dostosowanie metodologii działań do bieżącej sytuacji. Jesteśmy świadomi, że przenoszenie treści dezinformacyjnych na grunt polskojęzycznej części mediów społecznościowych na pewno stanowi wyzwanie także w 2023 r.

Kolejnym działaniem wpisującym się w przeciwdziałanie zagrożeniom związanym z cyberbezpieczeństwem jest zharmonizowanie na poziomie unijnym zasad zwalczania i zapobiegania materiałom przedstawiającym seksualne wykorzystanie dzieci, tj. CSAM (*Child Sexual Abuse Material*). Opowiadamy się za wspólnymi zasadami, w szczególności za obowiązkiem szacowania ryzyka w tym zakresie, usuwania materiałów CSAM oraz raportowania o takich materiałach unijnemu centrum, które ma być powołane. Aktywnie uczestniczymy w pracach w Radzie Unii Europejskiej nad nowym rozporządzeniem unijnym w sprawie zwalczania i zapobiegania materiałom CSAM. Podkreślamy, że prawo dzieci do życia, godności, integralności fizycznej i psychicznej czy bezpieczeństwa osobistego to niezwykle istotne wartości. Dlatego postrzegamy ochronę dzieci przed wykorzystywaniem seksualnym jako jeden z kluczowych obowiązków. Dostrzegamy potrzebę, aby nowe ramy regulacyjne dotyczące przeciwdziałania i zwalczania wykorzystywania seksualnego dzieci online były powiązane z istniejącymi mechanizmami i rozwiązaniami systemowymi w tym obszarze oraz spójne z zadaniami realizowanymi przez organy ścigania w zakresie wykrywania przestępstw i ścigania ich sprawców.

Chciałbym również zwrócić państwa uwagę na fakt, że działania w zakresie podnoszenia świadomości społecznej na tematy związane z zagrożeniami ze strony cyberprzestępczości są w Polsce podejmowane przez różne podmioty, zarówno przez organy ścigania, jak i poszczególnych ministrów kierujących działami czy organizacje pozarządowe. Zadania w zakresie podnoszenia cyberświadomości zostały przypisane ministrowi właściwemu do spraw informatyzacji oraz pełnomocnikowi rządu do spraw cyberbezpieczeństwa, niemniej nie można ich utożsamiać z zadaniami w zakresie ochrony obywateli przed cyberprzestępczością, w szczególności w obszarze dominującej kategorii zagrożeń, jakimi są oszustwa komputerowe. Zadania te są realizowane przez różne podmioty w zakresie ich właściwości rzeczowej.

Działalność ministra cyfryzacji skupia się na prewencji poprzez działania edukacyjne i uświadamiające. Oprócz realizowanych kampanii edukacyjno-informacyjnych konsekwentnie rozbudowywana jest ogólnodostępna baza wiedzy o cyberbezpieczeństwie na portalu gov.pl, gdzie zamieszczane są m.in. treści edukacyjne na temat różnych zagrożeń w sieci i zasad cyberhigieny, a także bieżące alerty dotyczące ostrzeżeń CERT Polska. Biuro Pełnomocnika Rządu do spraw Cyberbezpieczeństwa w grudniu 2022 r. uruchomiło kampanię w radiu i telewizji na temat zagrożeń związanych z fałszywymi SMS-ami oraz kampanię promującą poradnik „ABC cyberbezpieczeństwa". Ponadto w 2022 r. Biuro Pełnomocnika Rządu do spraw Cyberbezpieczeństwa prowadziło prace przygotowawcze do kampanii edukacyjno-informacyjnej, która zostanie zrealizowana w tym roku. Jest to działanie realizowane wspólnie z Departamentem Cyberbezpieczeństwa w KPRM oraz państwowym instytutem badawczym NASK w ramach projektu na rzecz upowszechniania korzyści z wykorzystywania technologii cyfrowych, współfinansowanego z programu „Polska Cyfrowa". Dziękuję państwu za uwagę.

Przewodniczący poseł Radosław Fogiel (PiS):

Bardzo dziękuję, panie ministrze.

Otwieram dyskusję. Zgłosił się pan poseł Arkadiusz Marchewka. Bardzo proszę, panie pośle.

Poseł Arkadiusz Marchewka (KO):

Dziękuję, panie przewodniczący. Szanowny panie ministrze, szanowni państwo, nie ma żadnych wątpliwości, że cyberwojna jest elementem tej wojny, która trwa za naszą wschodnią granicą. Po barbarzyńskim ataku putinowskiej Rosji na niepodległą Ukrainę działania dotyczące również ataków w cyberprzestrzeni zostały zintensyfikowane i po prostu są elementem wojny. Dlatego powinniśmy być przygotowani jak najlepiej na to, aby chronić nie tylko instytucje publiczne i infrastrukturę krytyczną, ale też obywateli przed zagrożeniami, które pojawiają się w związku z tymi tematami.

Jeśli chodzi o kwestie dotyczące infrastruktury krytycznej, strategicznej, to jest jedna sprawa, natomiast chciałbym zwrócić uwagę na to, w jaki sposób instytucje państwowe dbają i pomagają obywatelom, kiedy ci spotkają po prostu niebezpieczeństwo w sieci. Chciałbym się odnieść do raportu Najwyższej Izby Kontroli, który został przedstawiony dwa dni temu. Niestety wnioski z tego raportu są druzgocące, dlatego że wynika z nich jasno, że zwykli obywatele zostali pozostawieni samymi sobie albo po prostu rzuceni na pastwę cyberprzestępców. Jeśli chodzi o dane, które zostały przedstawione w raporcie, to z tych wszystkich ataków, które zostały odnotowane wśród osób ankietowanych, wynika, że 85% zakończyło się albo nieodnalezieniem sprawcy, albo umorzeniem sprawy, a jedynie 2% jakichkolwiek przestępstw w Internecie zakończyło się pozytywnie dla osób, które zostały tym dotknięte.

Pozwolą państwo, że przytoczę tylko kilka słów z ogólnej oceny, którą ten raport zawiera. Zacznę od tego, że NIK wskazuje, że – cytuję: „organy odpowiedzialne za bezpieczeństwo cyberprzestrzeni oraz koordynację polityki rządu w tym obszarze nie reagowały na identyfikowane ryzyka oraz zagrożenia i nie dostosowywały do nich swoich działań organizacyjnych i informacyjnych". Po drugie „w jednostkach Policji nie wypracowano instrukcji dla obywateli zgłaszających tego rodzaju zdarzenia, a algorytmy przyjmowania zgłoszeń przygotowane dla policjantów były z kolei wadliwe i stanowiły tylko ograniczone wsparcie dla funkcjonariuszy. Procedury zgłaszania i obsługi incydentów zostały wypracowane w NASK, jednakże tylko symboliczna liczba osób posiadała wiedzę na temat możliwości uzyskania wsparcia ze strony tego podmiotu". Co więcej, „NIK oceniła jako nierzetelne i nieskuteczne prowadzone w badanym okresie działania mające na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych, w tym kradzieży tożsamości".

Wnioski z tego raportu są wręcz druzgocące i pokazują jasno, że w badanym okresie obywatele mieli do czynienia raczej z cyberniebezpieczeństwem niż z cyberbezpieczeństwem. Mam nadzieję, że w ostatnich kilkunastu miesiącach, od kiedy

zakończono to badanie, sytuacja się poprawiła. Tak jak kwestie dotyczące ochrony infrastruktury krytycznej są w tym raporcie wskazywane jako chronione w sposób odpowiedni, tak te dotyczące sytuacji poszczególnych, po prostu zwykłych obywateli i użytkowników internetu, narażonych na ataki z każdej strony, są bardzo krytycznie oceniane.

Oczywiście okres badania kończy się na rozpoczęciu 2022 r., więc chciałbym zapytać pana ministra odpowiedzialnego za sprawy cyfryzacji, co przez ten rok od zakończenia tego badania zrobiono, aby poprawić bezpieczeństwo obywateli w sieci. To po pierwsze. Po drugie, czy zastosowano się do rekomendacji, które w raporcie NIK zostały zawarte? Dziękuję.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję. Bardzo proszę, panie ministrze.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Dziękuję bardzo. Przede wszystkim chciałem podkreślić, że kontrola dotyczyła lat 2019–2021, a jej wyniki zostały opublikowane 7 marca 2023 r., czyli zdaje się, że przedwczoraj. Dlatego w naszej ocenie publikacja raportu, który dotyczy zupełnie innej sytuacji, niż jest dzisiaj, jest jakimś rodzajem manipulacji czy wprowadzenia opinii publicznej w błąd. Dzisiaj, jak ktoś przeczytałby taki nagłówek, to pomyślałby, że stoimy w obliczu wojny i cyberzagrożenia, a przypominam, że zdaje się dwa miesiące temu Microsoft opublikował raport, z którego wynika, że Polska jest państwem najczęściej atakowanym przez inne podmioty państwowe. Czyli tutaj jakby mamy do wyboru zasadniczo dwa: jeden to Rosja, a drugi to niech państwo sobie sprawdzą. Natomiast sytuacja dzisiaj jest zupełnie inna. Jesteśmy po doświadczeniach COVID i po bardzo szybkiej ścieżce cyfryzowania w ogóle całego społeczeństwa w związku z sytuacją COVID-ową. Jesteśmy cały czas na bardzo wysokim poziomie alertów w związku z sytuacją za naszą wschodnią granicą. Stan faktyczny na dzień dzisiejszy w ogóle nie koresponduje z tym, co wtedy było publikowane.

Teraz tak. Kluczową kwestią, na którą chcielibyśmy zwrócić uwagę, jest projekt ustawy o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości. To jest pierwszy projekt, który wprowadziliśmy w tej sprawie. Wkrótce w aplikacji mObywatel będzie można zgłosić zastrzeżenie, że nie chcemy zaciągać zobowiązań finansowych. Nowe przepisy blokować będą możliwość dochodzenia roszczeń udzielonych pomimo dokonanego zastrzeżenia. Celem wprowadzenia tych zmian jest zmniejszenie liczby przestępstw z użyciem skradzionej tożsamości, a także ograniczenie strat wynikających z wyłudzeń i innych skutków takiej kradzieży.

Kolejnym bardzo ważnym krokiem w trosce o bezpieczeństwo użytkowników jest projekt ustawy o zwalczania nadużyć w komunikacji elektronicznej, który został już skierowany do Sejmu. Zgodnie z nowymi przepisami operatorzy będą musieli blokować SMS-y wyłudzające dane i połączenia głosowe, których celem jest podszywanie się pod inną osobę. To jest to, co mówiłem o *smishingu* i *phishingu*.

Kontrolerzy NIK przytoczyli także argumenty, które w ich ocenie stanowiły potwierdzenie tezy, że cyfryzacja, KPRM i NASK nie prowadziły wystarczającej kampanii edukacyjno-informacyjnej w zakresie przestępstw internetowych. W wynikach badań wzięto jednak pod uwagę zaledwie niewielką część działań realizowanych w ramach licznych, jak podkreśla NIK, kampanii komunikacyjnych, czyli sami sobie pokazują, że zauważyli tylko kilka, wiedząc, że jest ich mnóstwo. Takie przedstawienie tematów pokazuje niespójność raportu i rozbieżność wniosków, które zostały podane do wiadomości publicznej.

O tym, że świadomość w obszarze bezpieczeństwa rośnie, a kampanie edukacyjno-informacyjne przynoszą efekty, świadczy zgłaszalność incydentów w CERT Polska. W 2021 r. zespół reagujący CERT zarejestrował 116 tys. zgłoszeń od obywateli, a w 2022 r. już 322 tys. zgłoszeń. To znaczy, że ludzie zwiększyli swoją świadomość i wiedzą, gdzie mają raportować. Czyli to nie jest wiedza zastrzeżona tylko dla jakiejś wąskiej grupy ludzi, tak jak w raporcie zostało to wskazane. Widoczny jest trend wzrostowy.

Realizujemy, poza tym liczne kampanie, jak np. kampania skierowana do rodziców i opiekunów „Nie zagub dziecka w sieci". Powstała seria poradników dla rodziców, jak

i inne artykuły edukacyjne. Odbywały się także webinaria i wykłady z ekspertami. To seria animowanych filmów dla dzieci „Bądź z innej bajki". Kampania „e-Senior potrafi!" wprost i w przystępny sposób edukuje, informuje i pomaga osobom starszym poznawać cyfrowy świat. Publikowane poradniki, filmiki instruktażowe, artykuły i broszury pokazują, jak bezpiecznie korzystać z nowych technologii. Akcja „Seniorze – spotkajmy się w sieci", której celem jest zwiększenie wiedzy w zakresie bezpieczeństwa seniora w internecie, pokazuje metody wykorzystywane przez oszustów w sieci. „Cyberlekcje" to 18 scenariuszy lekcyjnych wraz z materiałami uzupełniającymi. Są infografiki, prezentacje, animacje, filmy z ekspertami itd. „Bezpieczni w sieci" to platforma e-learningowa przeznaczona dla nauczycieli i uczniów klas VII i VIII szkół podstawowych oraz szkół średnich, której celem jest wspieranie pedagogów i młodzieży oraz podnoszenie kompetencji cyfrowych.

Przypominamy, że stworzenie jednego modelowego procesu edukacji w obszarze cyberzagrożeń byłoby zupełnie nieskuteczne. Należy dostosować komunikaty i treści do poszczególnych grup docelowych, uwzględniając przy tym szereg zmiennych: wiek, poziom kompetencji cyfrowych, sposób korzystania z internetu. W zależności od odbiorcy budowane są narracja i komunikacja, których celem jest uwrażliwienie użytkowników na cyberzagrożenia, edukowanie w zakresie cyberbezpieczeństwa i zabezpieczenia urządzeń, z których korzystają oraz umiejętności poruszania się w sieci.

Wyjaśnić też należy poruszoną w raporcie NIK kwestię zarządzania systemem S46. System ten nie służy bezpośrednio do zwalczania cyberprzestępczości skierowanej przeciwko indywidualnym użytkownikom internetu. Jednym z głównych jego założeń jest to, że wymiana informacji w ramach systemu odbywa się nawet wtedy, gdy zakłócone będzie funkcjonowanie internetu lub publicznej sieci telefonicznej. Ta funkcjonalność systemu została w pełni osiągnięta. Natomiast wydatkowane środki, które NIK przytoczyła w raporcie, zostały przeznaczone na budowę i utrzymanie systemu bezpiecznej sieci. Naukowa i Akademicka Sieć Komputerowa pozyskała środki, które pozwolą na sfinansowanie połączeń 150 podmiotów do końca roku 2023. Wraz z uruchomieniem środków „Krajowego planu odbudowy" (KPO) przewidywane jest podłączenie do systemu kolejnych 400 podmiotów, głównie operatorów usług kluczowych, sektora ochrony zdrowia oraz jednostek samorządu terytorialnego.

Cyfryzacja i NASK nieustannie pracują nad poprawą cyberbezpieczeństwa, inicjując i przeprowadzając liczne warsztaty, szkolenia i kampanie edukacyjne dla wszystkich grup użytkowników. W tej chwili, nawet na dzień dzisiejszy, już nie będziemy tego ogłaszać, ale w najbliższym czasie będą specjalne kampanie, kursy, szkolenia i dedykowane programy, np. dla kobiet, dla osób starszych, dla poszczególnych kategorii społecznych, które mogą być narażone na cyberzagrożenia.

Jeśli są jeszcze jakieś pytania, to oczywiście jestem otwarty. Dziękuję bardzo.

Poseł Arkadiusz Marchewka (KO):

Przepraszam, panie ministrze. A czy mógłbym poprosić o odpowiedź na piśmie? Jakie działania podjęto od czasu zakończenia badania przez NIK po to, aby zniwelować ewentualne skutki cyberataków na obywateli?

Podsekretarz stanu w KPRM Paweł Lewandowski:

Oczywiście przekażemy.

Poseł Arkadiusz Marchewka (KO):

Dziękuję.

Przewodniczący poseł Radosław Fogiel (PiS):

Pan poseł Konrad Frysztak się zgłaszał jako następny.

Poseł Konrad Frysztak (KO):

Dziękuję, panie przewodniczący. Wysokie Komisje, panie ministrze, dwa miesiące temu Komisja Europejska wprowadziła dyrektywę w sprawie odporności podmiotów krytycznych (dyrektywa CER), która – poza określeniem podmiotów strategicznych dla funkcjonowania kraju – ma również skatalogować zasób wynikający z cyberbezpieczeństwa. Chciałbym zapytać, czy u ministra cyfryzacji toczą się już prace

zmierzające do tego, by nakreślić, które podmioty zostały wskazane jako krytyczne dla bezpieczeństwa. Czy pracują państwo w tym międzyresortowym zespole, który – z tego, co wiem – chyba już został powołany, aby również współpracować z innymi krajami UE?

Pragnę przypomnieć, że czas na implementację tych przepisów to 21 miesięcy od dnia wejścia w życie. Co za tym idzie, ten termin zbiegnie w październiku 2024 r., choć uważam, że powinien być jak najbardziej skrócony w związku z sytuacją za naszą wschodnią granicą i z tym, co dzieje się z bezpieczeństwem. Przypomnę, że również strony Sejmu i Senatu były swego czasu atakowane. Co za tym idzie, cyberbezpieczeństwo powinno być dzisiaj jedną z najważniejszych domen zabezpieczenia naszego kraju.

Przewodniczący poseł Radosław Fogiel (PiS):

Panie ministrze, proszę uprzejmie.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Dziękuję bardzo. Minister cyfryzacji i pełnomocnik rządu do spraw cyberbezpieczeństwa nie są bezpośrednio odpowiedzialni za implementację tej dyrektywy. Dyrektywą zajmuje się Rządowe Centrum Bezpieczeństwa. Oczywiście trwają już prace. Zespół, o który pan zapytał, funkcjonuje. Oczywiście nam też zależy, by jak najszybciej wdrożyć przepisy, które są tam zawarte, ale chciałem zwrócić uwagę, że przepisy to jest jakby jedna strona medalu, natomiast działania, które podejmujemy niezależnie od tych przepisów, to jest zupełnie inna sprawa. Oczywiście im szybciej te przepisy będą, tym lepiej, ale brak tych przepisów nie przeszkadza nam w prowadzeniu skutecznych działań w celu zabezpieczenia polskiej cyberprzestrzeni.

Natomiast jeśli chodzi o kwestie dotyczące stron internetowych, to należy pamiętać, są one najbardziej efektownym sposobem działania hakerów, ale w gruncie rzeczy są one stosunkowo mało skuteczne, albowiem poza podmianą treści na stronie rzadko wywołują inne negatywne skutki w postaci jakichś istotnych wycieków danych, które są w zupełnie innych piaskownicach umieszczone. W związku z tym wygląda to rzeczywiście niedobrze, ale zapewniam państwa, że w większości przypadków to jest trochę jak wybicie cegłą szyby w sklepie. Dużo huku, dużo hałasu, ale poza tym szczególnego zagrożenia najczęściej nie wywołuje.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję bardzo. Tak? Jeszcze raz.

Poseł Konrad Frysztak (KO):

Słowem dopytanie, ponieważ na posiedzeniu podkomisji we wtorek RCB przedstawiało chociażby podmioty, które… Może nie wprost z nazwy, ale ile podmiotów wskazanych zostało przez Ministerstwo Obrony Narodowej. Mam pytanie. Ile pan minister wskazał tych podmiotów, które są strategiczne ze względu na bezpieczeństwo?

Podsekretarz stanu w KPRM Paweł Lewandowski:

Ponieważ nie wiedziałem, że to będzie dzisiaj przedmiotem tego posiedzenia Komisji, to nie mam przygotowanej odpowiedzi. Przygotuję dla pana na piśmie.

Poseł Konrad Frysztak (KO):

Bardzo dziękuję.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję. Czy ktoś z państwa posłów jeszcze ma pytania? Jeśli nie, to czy mają je zaproszeni goście? Bardzo proszę.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Dzień dobry. Nazywam się Joanna Karczewska. Reprezentuję osoby, które na co dzień zajmują się cyberbezpieczeństwem, bezpieczeństwem, informacją, ochroną danych osobowych. Z uwagą wysłuchałam dzisiejszej dyskusji. Mam trzy kwestie, które chciałabym poruszyć.

Pierwsza jest niespójność przepisów, które później rzutują na wręcz zagrożenie dla cyberbezpieczeństwa. Takim przykładem jest chociażby konwencja w sprawie unikania podwójnego opodatkowania i zapobiegania uchylaniu się od opodatkowania.

Jest to konwencja podpisana pomiędzy RP a Stanami Zjednoczonymi. Tam jest mowa o tym, że Ministerstwo Finansów i Krajowa Administracja Skarbowa będą automatycznie przekazywać dane pozyskane z banków, jeżeli banki stwierdzą, że ktoś się uchyla od opodatkowania. Tyle że, swoją drogą, niezależnie od tego MSZ podpisało ze Stanami Zjednoczonymi stosowne dokumenty, które wprowadzają wyjątki od zapisów konwencji. Finał jest taki, że dochodzi do bezprawnego, nielegalnego i automatycznego przekazywania danych obywateli RP. Niestety brak na to reakcji ze strony odpowiednich organów państwa. To jest jeden przykład. Inne przykłady zawieram regularnie w swoich artykułach, które publikuję w kwartalniku Polskiego Towarzystwa Informatycznego. Polecam lekturę, bo przykładów jest naprawdę dużo.

Druga kwestia. Pominął pan, panie ministrze, chociażby akcję weryfikacji bezpieczeństwa w szpitalach. Wiem, że to nie jest prowadzone przez ministra cyfryzacji, tylko przez Ministerstwo Zdrowia w połączeniu z Narodowym Funduszem Zdrowia, ale to jest porównywalne z tym, co się dzieje w gminach czy w powiatach. Zastosowano tam zupełnie inne kryteria oceny. Warto to porównać. Dokonałam tego właśnie w jednym ze swoich artykułów. Wnioski są bardzo ciekawe. Polecam pana uwadze.

Trzecia rzecz to jest uświadamianie. Tak, też czytałam raport. Właściwie to mogę powiedzieć, że jestem ekspertem zewnętrznym, który uczestniczył w opracowaniu raportu razem z NIK. Od tego czasu uważnie śledzę, jak wyglądają zmiany w budowaniu uświadamiania i we wszelkich akcjach informacyjnych. W związku z tym mam do pana ministra pytanie. Co by pan polecił woźnej w przedszkolu? Gdzie ma zajrzeć do internetu, żeby się dowiedzieć, jakie są zagrożenia przestępczością w Internecie? Na co ma zwrócić uwagę? Z jakim materiałem się zapoznać? To byłoby bardzo ciekawe dla mnie, ponieważ akurat to jest grupa, która chyba została pominięta w całej akcji.

Kolejna sprawa to seniorzy. Wielokrotnie już zadawałam pytanie na posiedzeniach Komisji, dlaczego seniorzy informatycy nie są wykorzystywani do akcji dla seniorów. Mamy wiedzę, mamy doświadczenie, na dodatek mamy siwy włos na skroni, a to sprawia, że dystans pomiędzy seniorami edukowanymi a seniorami edukatorami jest dużo mniejszy. Potrafimy nawiązać inną więź z seniorami niż – powiedzmy – młodzi ludzie. Pragnę zauważyć, że na posiedzeniach innej komisji sejmowej była bardzo ciekawa prezentacja tego, co robią związki emerytów i rencistów wspólnie z Policją. Panowie wiedzą o tym, że tam akurat doszli do porozumienia i emerytowani policjanci są wykorzystywani do prowadzenia akcji uświadamiających wśród seniorów. To bardzo dobra inicjatywa. Mam nadzieję, że również seniorzy informatycy będą w ten sposób wykorzystani.

Ostatnia sprawa. Właśnie sprawdziłam w raporcie współpracę międzynarodową. W wystąpieniach i pana ministra, i pana ministra z MSZ zabrakło mi również zaznaczenia, jak wygląda współpraca z organizacjami międzynarodowymi, które zajmują się cyberbezpieczeństwem i zwalczaniem cyberprzestępczości na co dzień. Taką organizacją jest moja ISACA. Międzynarodowa organizacja, która jako jedyna na świecie certyfikuje audytorów systemów informatycznych. Właśnie trwają prace nad kolejnymi dokumentami w ramach nowej metodyki pozwalającej wprowadzić i utrzymać tzw. *digital trust*, czyli zaufanie do cyfryzacji, a jest to dzisiaj temat najważniejszy. Skoro nasze życie się przenosi do cyberprzestrzeni, to ważne jest, a właściwie kluczowe, żebyśmy mogli ufać temu, co tam się dzieje. Dobrym przykładem jest chociażby akcja e-PIT. Przez wiele lat MF budowało zaufanie do e-PIT i dzisiaj bardzo dużo osób się decyduje na automatyczne akceptowanie e-PIT. Wynika to właśnie z zaufania. Teraz duże wyzwanie dla MF, żeby to zaufanie utrzymać, żebyśmy nadal wierzyli w to, że będzie to bezpieczne. Generalnie jednak właśnie zabrakło mi zaznaczenia, jak wygląda współpraca z międzynarodowymi organizacjami, które zrzeszają specjalistów od cyberbezpieczeństwa, bezpieczeństwa, informacji, ochrony danych osobowych. Dziękuję.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję. Czy pan minister chciałby się odnieść do tych kwestii – nie wiem – unikania podwójnego opodatkowania czy tej umowy?

Podsekretarz stanu w MSZ Paweł Jabłoński:

Nie usłyszałem żadnego pytania do MSZ, więc trudno mi… Temat jest bardzo kompleksowy. Oczywiście można byłoby się do tego odnosić, chociaż kompetencyjnie to jest bardziej w zakresie MF, jeśli chodzi o podwójne opodatkowanie. W pozostałym zakresie to jest właściwy resort.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję. Panie ministrze, czy pan do czegoś chciałby się odnieść?

Podsekretarz stanu w KPRM Paweł Lewandowski:

Dziękuję. Panie przewodniczący, Wysokie Komisje, chciałem zwrócić uwagę na tę kwestię, którą poruszyła pani ekspert, a dotyczącą edukacji seniorów. My oczywiście to dostrzegamy i absolutnie zgadzamy się z diagnozą, że dużo łatwiej jest prowadzić edukację, jeśli to seniorzy edukują, dlatego wspieramy cyfrowe kluby seniora. Zdaje się, że w zeszłym roku wydaliśmy prawie 12 mln zł na działania związane z podniesieniem wiedzy dotyczącej cyberbezpieczeństwa i cyfryzacji, dedykowane wyłącznie cyfrowym klubom seniora. Takie działania będziemy prowadzić także w tym roku i w kolejnych iteracjach tego procesu.

Jeśli chodzi o inne kwestie, one często jednak dotyczą rzeczy niezwiązanych bezpośrednio z KPRM i cyfryzacją. Były tutaj poruszone kwestie dotyczące ministra zdrowia i jego działań prowadzonych w zakresie zabezpieczenia danych. Była zwrócona uwaga na jakąś kwestię, że coś jest niespójne.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Nie. Jeżeli mogę, nie to… Zabrakło mi właśnie tylko tego, że wiecie o tym, że równolegle do „Cyfrowej Gminy" i „Cyfrowego Powiatu" ma miejsce ta sama akcja, ale prowadzona przez inny resort właśnie w szpitalach, co jest równie cenną inicjatywą jak to, co robicie dla gmin i powiatów.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Przyjąłem. OK. W każdym razie wiemy, że taka akcja ma miejsce, tylko trzeba pamiętać, że każdy resort także w swoim zakresie… Ponieważ cyfryzacja jest horyzontalnym przedsięwzięciem, to każdy resort w swoim zakresie musi także prowadzić swoje działania, biorąc pod uwagę specyfikę nadzorowanego obszaru. Praktycznie każdy resort ma taki departament, który jest z nami w dialogu. Jeśli trzeba prowadzić jakieś działania wspólne, to jest Komitet Rady Ministrów do spraw Cyfryzacji (KRMC), któremu przewodniczę. Takie kwestie również są podnoszone podczas jego obrad. Mamy środki koordynacji działań dotyczących cyfryzacji *sensu largo*, a to jest też jeden z tych elementów, więc staramy się wspólnie działać, by podnieść świadomość i bezpieczeństwo.

Innych kwestii bezpośrednio do nas skierowanych nie zauważyłem. Jeśli takie są, to proszę… Aha, baza wiedzy. Pytała się pani, co poradzę woźnej w szkole.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Tak, woźnej w przedszkolu, która także korzysta z technologii, bo ma smartfona.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Tak. Na stronie gov.pl, czyli na naszej stronie rządowej, jest baza wiedzy o cyberbezpieczeństwie. Wystarczy wpisać „cyberbezpieczeństwo" na naszej stronie gov. pl. Wyświetli się bezpośrednie odniesienie do danych dotyczących cyberbezpieczeństwa. Tam jest cała baza wiedzy. Każdy aspekt wytłumaczony jest językiem ludzkim. Nie potrzeba mieć żadnej dodatkowej wiedzy technicznej, żeby zrozumieć kwestie, które tam są opracowane specjalnie dla każdego obywatela. Dziękuję bardzo.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję bardzo. Proszę bardzo, kolejny głos w dyskusji.

Wiceprezes Polskiej Izby Radiodyfuzji Cyfrowej Jacek Kosiorek:

Dzień dobry. Jacek Kosiorek z Polskiej Izby Radiodyfuzji Cyfrowej. Mam jeszcze pytanie do pana ministra, jeżeli mogę.

Martwi mnie jedna rzecz, ponieważ przyglądam się liczbie aplikacji, które są instalowane na smartfonach czy urządzeniach, które mają Androida w Polsce. Część z tych aplikacji wysysa nadmierną ilość danych od klientów. To jest problem, bo uważam, że należałoby… Może to jest też taka sugestia. Rodzaj sprzętu jednej z chińskich firm, który nie jest promowany jako niebezpieczny dla klientów, był podany w mediach, co mnie cieszyło, jako ewentualne zagrożenie dla bezpieczeństwa danych, które są w jakiś sposób wysysane. Natomiast chodzi o aplikacje, które ewentualnie np. słuchają nas w tej chwili i analizują ten tekst jako język maszynowy. Czy w tym temacie też państwo jako ministerstwo powinni coś zrobić? Dziękuję.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Jeśli chodzi o aplikację, o której pan wspomniał, to oczywiście trzeba pamiętać, że przede wszystkim aplikacje, które ściągamy, muszą być z pewnego źródła. Niezależnie od tego musimy oczywiście sami zwrócić uwagę na wiele rzeczy. To jest też odpowiedzialność dostawców, tych sklepów internetowych. Mamy zasadniczo dwóch wiodących, ale w przypadku Androida to przede wszystkim jest sklep Google. Odpowiedzialność leży też po ich stronie. Dlatego że liczba aplikacji, które się pojawiają, jest tak olbrzymia, że domyślam się, jak trudno jest też to wszystko kontrolować, żeby dać rękojmię, a poza tym jedna aplikacja przez kilka lat może funkcjonować zupełnie przyzwoicie, a w kolejnym updacie nagle zaczyna… Wiedzą państwo, że są działania przestępcze, którym bardzo trudno jest tak po prostu przeciwdziałać. Trzeba stosować prewencję bardziej na poziomie edukacji, bo trudno jest prewencyjnie nagle blokować aplikację, która jeszcze nic złego nie robi, a w przyszłości może coś robić. Dopóki te rzeczy są zgodne z prawem i z regulaminami podmiotów, które świadczą te usługi, a podmioty te działają zgodnie z prawem, to jest to bardzo trudne. Opierałbym się tu przede wszystkim na edukacji.

A drugie pytanie? Dotyczyło… Mógłby pan powtórzyć?

Wiceprezes PIRC Jacek Kosiorek:

Na szczęście w pewnym momencie to podano, bo są właśnie urządzenia, które z założenia i tak jakby z poszerzenia – szczególnie chodziło o routery i sprzęt IT – wedle osób zajmujących się IT są niebezpieczne. Czyli zakładamy, że…

Podsekretarz stanu w KPRM Paweł Lewandowski:

Aha, rozumiem. Chodzi o to, że dostawcy niektórych sprzętów mają możliwość wgrywania do nich softu, który mógłby potencjalnie zbierać dane o ruchu, dane o odwiedzanych witrynach.

Wiceprezes PIRC Jacek Kosiorek:

Na przykład. Tam była wymieniona jedna z firm. Nie chcę jej wymieniać w tej chwili, celowo właśnie omijam, ale w tym momencie uważam, że chodzi również o zwrócenie uwagi w przyszłości na to, żeby dany sprzęt tak jakby był omijany przez pewne grupy.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Oczywiście, że są pewne firmy, które mogą być postrzegane jako bardziej ryzykowne. Natomiast trzeba pamiętać, że zasadniczo każdy producent ma możliwość wgrywania za pomocą poprawek, updatu itd. oprogramowania, które w kolejnej swojej iteracji może zawierać dodatkowe funkcje przez nas niepożądane.

Trudno jest podmiotom państwowym bez jakiegoś szczególnego mechanizmu na dzień dzisiejszy po prostu wyjść i powiedzieć, że ta czy inna firma jest szczególnie niebezpieczna i nie rekomendujemy zakupów, bo wtedy naruszamy i umowy o wolnym handlu, i umowy międzynarodowe z podmiotami trzecimi, gdzie te firmy są zarejestrowane. Zaburzamy prawo konkurencji, mnóstwo przepisów unijnych dotyczących dyskryminacji, więc to jest bardzo trudny temat. Słusznie, że pan zwrócił na to uwagę, natomiast tutaj musielibyśmy za każdym razem podejmować działania na poziomie unijnym i to tylko w bardzo ograniczonym zakresie.

W przypadku procedowanej u nas ustawy dotyczącej krajowego systemu cyberbezpieczeństwa określamy, że przy niektórych typach świadczenia usług muszą być urządzenia, które mają jakiś rodzaj certyfikacji. Natomiast ta ustawa jest jeszcze

procedowana i trochę czasu minie zanim ona wejdzie w życie, ale w tym zakresie ona będzie dotyczyła tylko dostawców usług, a nie sprzętu używanego przez podmioty, przez użytkowników prywatnych.

Tak jak powiedziałem, czekamy na uregulowania unijne. W tej chwili są prowadzone prace nad specjalnie dedykowanym rozwiązaniem. Jest rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020. Dopiero te przepisy dadzą nam jakieś zharmonizowane możliwości takiego prowadzenia działań, byśmy mogli powiedzieć, że działamy zgodnie z zasadami UE.

Wiceprezes PIRC Jacek Kosiorek:

Dziękuję serdecznie.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję bardzo. Czy jeszcze są jakieś zgłoszenia? Jeśli nie, to pozwolę sobie tylko jeszcze na jedno pytanie. Panie ministrze, myślę, że na tym będziemy kończyć, bo rzeczywiście to, od czego pan tutaj zaczął, czyli…

W takiej dyskusji dzisiaj nie można abstrahować od kontekstu wojny na Ukrainie. Chciałem zapytać bez szczegółów, ale jeśli chodzi o statystyki rozmaitych ataków, czy to na infrastrukturę, czy wyłudzania danych, jak państwo to oceniają. Jak państwo to widzą? Czy w ciągu ostatniego roku widać znaczący wzrost takich ataków, które można powiązać z agentami państwowymi, a nie tylko prywatnymi hakerami?

Druga sprawa. Jeśli chodzi o samą dezinformację, to oczywiście budowanie zbiorowej odporności jest tutaj bardzo ważne. Czy państwo prowadzą jednak jakieś działania analityczne, które miałyby na celu identyfikację źródeł, sposobów rozprzestrzeniania się, ścieżek, jakichś hubów, gdzie ta dezinformacja się rozchodzi? Chciałbym jeszcze zapytać o takie dwie rzeczy.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Zacznę może od drugiego pytania, jeśli pan przewodniczący pozwoli. Oczywiście prowadzimy takie działania. Prowadzi je NASK. Prowadzą je także służby. Cała ta działalność jest również koordynowana i na naszym poziomie KPRM i cyfryzacji oraz przez pełnomocnika rządu do spraw bezpieczeństwa informacyjnego w cyberprzestrzeni, który tworzy raporty z informacjami dotyczącymi właśnie m.in. tego, jaka narracja w jakim zakresie jest obecnie rozpowszechniana, jakie są jej źródła. Po prostu syntetyzuje informacje dostarczane przez cały szereg podmiotów, które mają w obowiązku monitorowanie lub raportowanie, jeśli się na takie działania natkną. Oczywiście ta wiedza u nas jest i jeśli są jakieś szczegółowe kwestie, to na piśmie możemy to przekazać na ręce pana przewodniczącego, w zależności od tego, w jakim zakresie możemy te dane udostępniać.

Jeśli chodzi o pierwszą kwestię, która dotyczyła statystyk, to wolelibyśmy też na piśmie… Natomiast oczywiście był moment dramatycznego wzrostu takiej działalności. W tej chwili ona się stosunkowo ustabilizowała na określonym poziomie. Główne kierunki ataku są znane. To Rosja i kraje wspierające, jawnie lub niejawnie, Rosję. Oczywiście wiemy, w jaki sposób ją wspierają i z jakich kierunków te ataki przychodzą. Natomiast trzeba pamiętać, że działamy. Wydaje mi się, że dosyć skutecznie odpieramy te ataki. Dziękuję bardzo.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję bardzo. Oczywiście, to w takim razie bylibyśmy wdzięczni. To, co można w trybie otwartym przekazać na piśmie, to z przyjemnością.

Jeszcze pan poseł Marchewka się zgłaszał.

Podsekretarz stanu w KPRM Paweł Lewandowski:

Panie przewodniczący, jeszcze tylko chciałem dodać, że będziemy mieć za chwilę raport CERT i on będzie jawny. W tym raporcie będziemy mieć pewnie cały system informacji, których pan przewodniczący oczekuje.

Przewodniczący poseł Radosław Fogiel (PiS):

Rozumiem. W takim razie się zapoznamy.

Bardzo proszę, panie pośle.

Poseł Arkadiusz Marchewka (KO):

Dziękuję. Panie ministrze, chciałbym jeszcze zapytać o jedną kwestię, dotyczącą ustawy o krajowym systemie cyberbezpieczeństwa, dlatego że proces trwa od 2020 r. Może to jeszcze nie nowelizacja, ale nazwijmy to konsultacjami zmian itd. Generalnie zostało to ujawnione w wykazie prac legislacyjnych. Niedawno, bo w tym roku. Jakie są dalsze losy prac nad tą ustawą? Kiedy możemy się spodziewać ostatecznego dokumentu? Kiedy Rada Ministrów się tym zajmie? Jak pan przewiduje, kiedy to może do Sejmu trafić?

Podsekretarz stanu w KPRM Paweł Lewandowski:

Dziękuję, panie pośle. Panie przewodniczący, Wysokie Komisje, rzeczywiście, jak to pan ujął, ujawniliśmy, że uruchomiliśmy ścieżkę legislacyjną dla tej ustawy. Ponieważ wnosi ona dosyć daleko idące konsekwencje dla wielu użytkowników i podmiotów działających na rynku, więc wiele podmiotów i użytkowników zgłasza mnóstwo uwag, które musimy rozpatrywać, żeby nie wylać dziecka z kąpielą. To jest trudna legislacja. Dotyczy wrażliwych kwestii. Chcielibyśmy, żeby jak najlepiej adresowała wyzwania, które przed nami stoją. Trzeba pamiętać, że w przypadku takich ustaw należy jak najbardziej i jak najlepiej je przekonsultować, by z jednej strony potem nie było żadnych wątpliwości co do intencji, jakie stoją za poszczególnymi przepisami, a z drugiej strony, by nie utrudnić również działania rynku czy normalnego funkcjonowania tych użytkowników, którzy na co dzień będą stykali się z podmiotami i infrastrukturą objętą przepisami tejże ustawy.

Jeśli chodzi o przewidywany kalendarz, właściwie to trudno mi powiedzieć. Na pewno w tej kadencji Sejmu będziemy chcieli tę ustawę uchwalić. Będziemy starać się jak najszybciej, bo rzeczywiście już ona jest dla nas też niezbędna z różnych innych powodów, toczących się innych procesów legislacyjnych i innych procesów regulacyjnych, które są. Dziękuję bardzo.

Poseł Arkadiusz Marchewka (KO):

Pozwoli pan, że tylko uzupełnię. Rzeczywiście, jeżeli mamy do czynienia z konfliktem za naszą wschodnią granicą, a wiemy, że cyberzagrożenia są jednymi z tych, które w sposób istotny dotykają użytkowników polskiego internetu, to zagwarantowanie działań czy przyjęcie nowelizacji ustawy powinno odbyć się jak najszybciej. Tutaj więc zbędna zwłoka w żaden sposób nie jest potrzebna, a wręcz wymagane jest, aby natychmiast, czy jak najszybciej te prace zostały podjęte, więc… Panie ministrze, oczywiście proces legislacyjny w Sejmie to jest coś, co jest na tym ostatecznym etapie. Ale jak pan zakłada? Gdyby tylko mógł pan powiedzieć, kiedy Rada Ministrów może to przyjąć, bo oczywiście przejście przez proces legislacyjny w Sejmie, a później w Senacie, trochę potrwa, ale kluczowe jest, kiedy z rządu wyjdzie ten ostateczny dokument. Czy mniej więcej spodziewa się pan, że stanie się to jeszcze w tym półroczu?

Podsekretarz stanu w KPRM Paweł Lewandowski:

Odpowiadając od końca, tak, oczywiście jestem przekonany, że to będzie jeszcze w tym półroczu. Największym problemem jest w pewnym sensie logistyka, tzn. liczba uwag, przygotowanie raportu z konsultacji, przygotowanie dokumentów, gdzie będziemy musieli się też ustosunkować do pewnych rzeczy. To jest najbardziej czasochłonne. No i cały czas rozmowy z podmiotami, które bezpośrednio będą objęte tymi przepisami.

Trzeba pamiętać, że ustawa o krajowym systemie cyberbezpieczeństwa funkcjonuje. To jest nowelizacja, więc to nie jest tak, że nie mamy ram prawnych, by chronić obywateli. A poza tym ta ustawa bezpośrednio nie dotyczy samych obywateli. Dotyczy ona podmiotów świadczących określone usługi, więc w jakiś tam pośredni sposób dotyczy obywateli, natomiast to nie jest tak, że przepisy nam przeszkadzają w realizowaniu zadań dotyczących ochrony obywateli na terenie RP przed cyberzagrożeniami. Brak określonych rozwiązań nie utrudnia nam codziennej ochrony obywateli. Natomiast, tak jak powiedziałem, jak najszybciej będziemy chcieli przyjąć określone przepisy.

Przewodniczący poseł Radosław Fogiel (PiS):

Dziękuję serdecznie. Jeśli nie ma więcej zgłoszeń w dyskusji, a takich nie widzę, stwierdzam, że Komisje zapoznały się z przedstawioną informacją.

Porządek obrad został na tym wyczerpany. Protokół dzisiejszego posiedzenia zostanie wyłożony do przejrzenia w sekretariatach Komisji. Zamykam posiedzenie naszych Komisji. Serdecznie państwu dziękuję.